

Chapter 1 - Introduction to Networks

#StudyGuideN10-009

#network

Chapter 1 - Introduction to Networks

Domain 1.0: Networking Concepts

Objective 1.6: Compare and contrast network topologies, architectures, and types



Chapter 1

Introduction to Networks

THE FOLLOWING COMPTIA NETWORK+ EXAM OBJECTIVES ARE COVERED IN THIS CHAPTER:

- ✓ Domain 1.0 Networking Concepts
- ✓ 1.6 Compare and contrast network topologies, architectures, and types.
 - Mesh
 - Hybrid
 - Star/hub and spoke
 - Spine and leaf
 - Point to point
 - Three-tier hierarchical model
 - Core
 - Distribution
 - Access
 - Traffic flows
 - North-south
 - East-west

1. Introducción

En la actualidad, la conectividad entre equipos es un elemento esencial tanto a nivel personal como profesional. Nuestra sociedad depende de la capacidad para **crear y mantener redes sólidas y fiables**, las cuales permiten compartir recursos, comunicarse y acceder a servicios distribuidos en distintos lugares.

Las redes pueden variar enormemente en tamaño y complejidad: desde una pequeña red doméstica hasta complejas infraestructuras corporativas globales. Sin embargo, todas ellas comparten la necesidad de estar **bien diseñadas, administradas y mantenidas**.

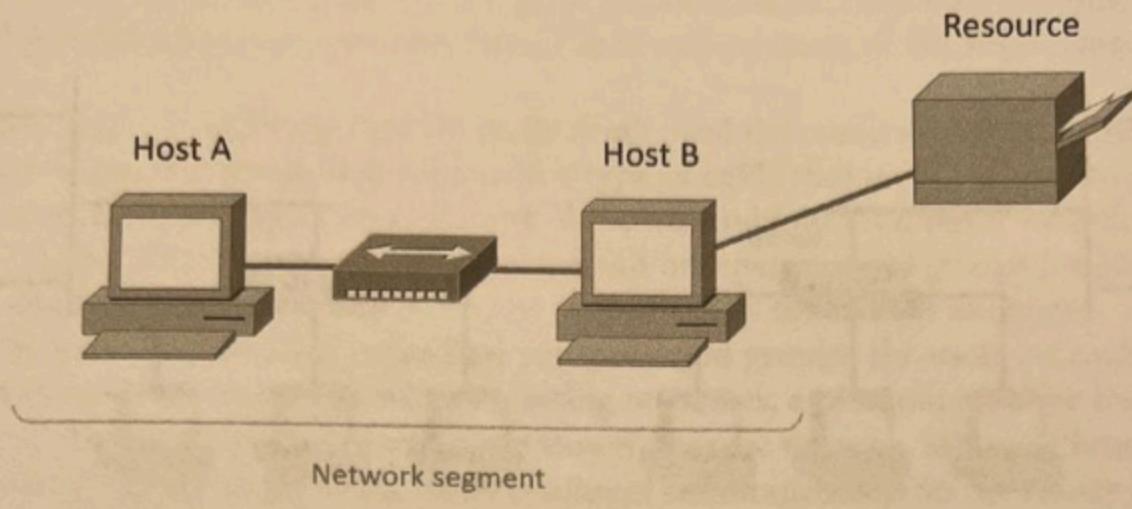
El objetivo de este capítulo es establecer los fundamentos del **networking**, presentando los tipos de redes, sus componentes, topologías, y conceptos arquitectónicos clave que forman la base del conocimiento necesario para el examen *CompTIA Network+*.

2. ¿Qué es una red?

Según la definición general, una **red (network)** es un grupo o sistema de personas o cosas interconectadas. En el contexto informático, se refiere a **dos o más computadoras conectadas que comparten recursos**, como datos, aplicaciones, impresoras o conexión a Internet.

Una red básica puede representarse mediante dos equipos conectados directamente que comparten archivos o periféricos. Estos equipos intercambian información usando un lenguaje binario de 1s y 0s, lo que constituye la base de toda comunicación digital.

FIGURE 1.1 A basic network

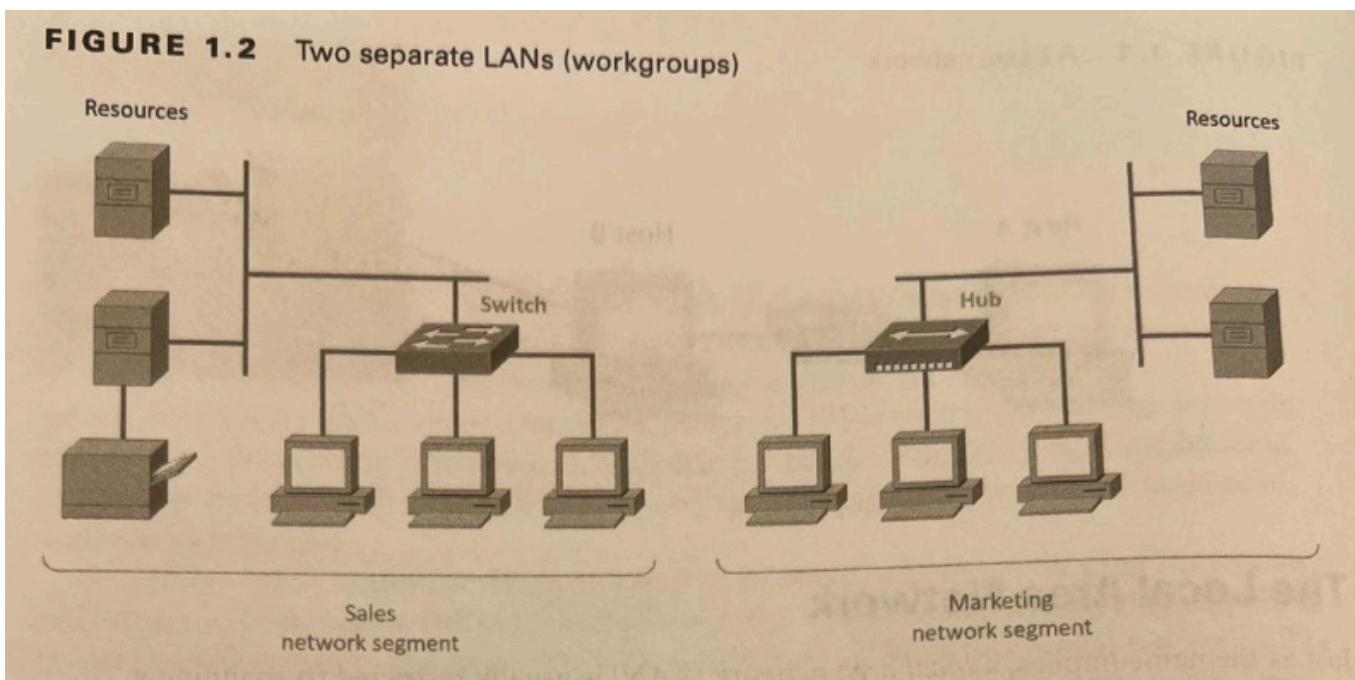


 **Ejemplo:** Dos hosts conectados mediante un cable Ethernet pueden intercambiar archivos o acceder a un recurso compartido, como una impresora de red.

3. Local Area Network (LAN)

Una **LAN (Local Area Network)** es una red que abarca un área geográfica limitada, como un edificio, un departamento o una vivienda. Las LAN permiten la conexión de múltiples dispositivos para compartir recursos de forma local.

En sus orígenes, las LAN tenían limitaciones de tamaño (por ejemplo, un máximo de 30 estaciones de trabajo), pero hoy en día la tecnología permite redes locales de mayor tamaño y flexibilidad. No obstante, sigue siendo habitual dividir grandes LAN en **zonas lógicas** llamadas *workgroups* para facilitar la administración.



- ◆ **Workgroup:** conjunto de dispositivos que pertenecen a la misma red física, sin una relación de dominio o control centralizado.
- ◆ **Domain:** entorno gestionado con un servidor que autentica y controla los dispositivos del grupo.

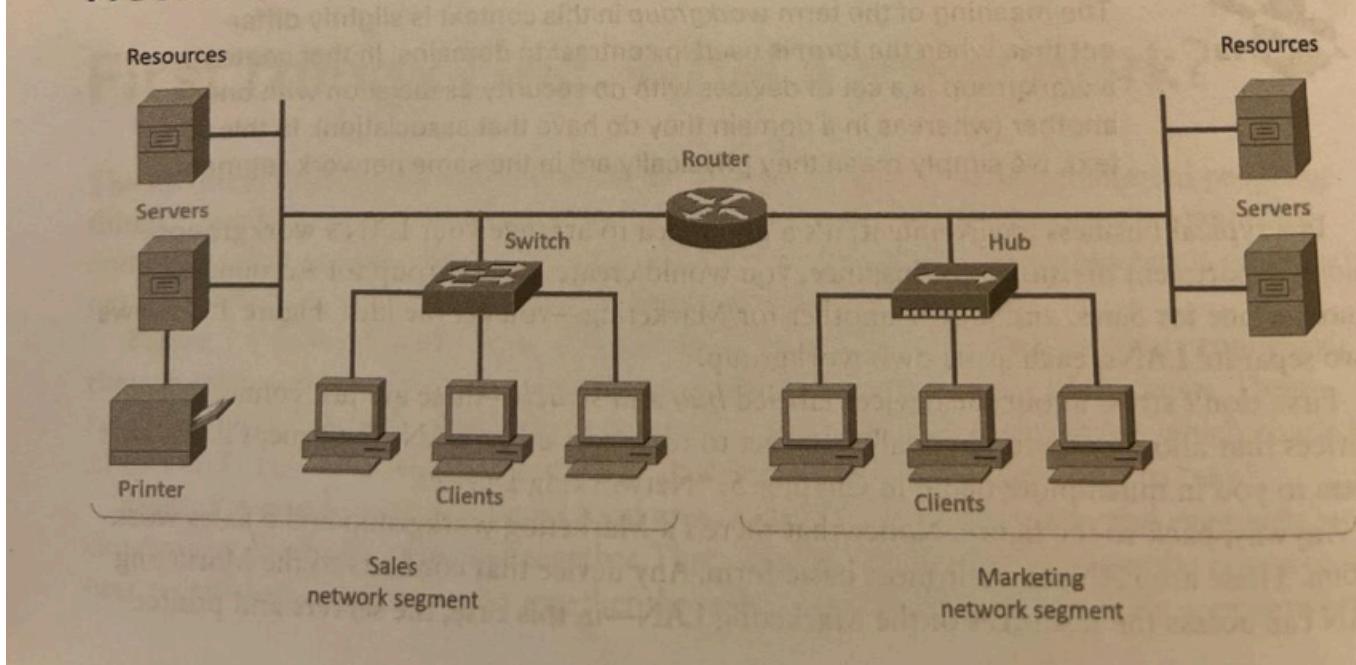
4. Estructura típica de una LAN

En un entorno empresarial, las LAN suelen organizarse por departamentos (por ejemplo, Ventas o Marketing), creando *workgroups* independientes. Cada grupo puede tener su propio segmento de red, y todos se interconectan mediante un **router** para compartir recursos entre ellos.

Ejemplo visual:

- Una LAN de Ventas con su propio switch y servidor de archivos.
- Una LAN de Marketing conectada mediante un hub.
- Un router que enlaza ambas redes, permitiendo que los equipos compartan recursos (por ejemplo, impresoras o servidores).

FIGURE 1.3 A router connects LANs



Esta estructura favorece:

- **Rendimiento**, ya que cada grupo maneja su propio tráfico.
- **Seguridad**, al segmentar el acceso.
- **Escalabilidad**, permitiendo añadir nuevos grupos o departamentos fácilmente.

5. Componentes comunes de una red

Las redes están compuestas por diferentes máquinas, dispositivos y medios que facilitan la

comunicación. Los tres elementos básicos son:

◆ **Workstations**

Equipos potentes utilizados por los usuarios finales. Suelen tener uno o más procesadores y recursos compartidos con otros usuarios de la red.

 No confundir con *client machines*: aunque se usan de forma intercambiable, el término *workstation* se refiere al sistema físico mientras que *client* describe su rol dentro de la red.

◆ **Servers**

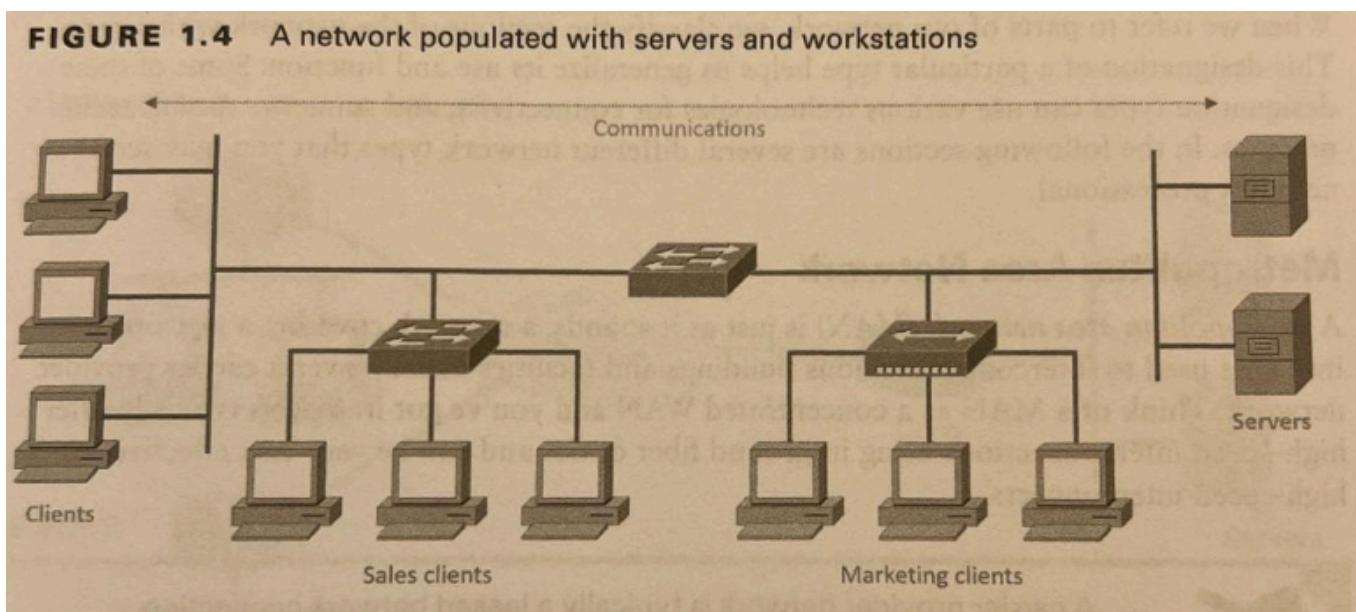
Computadoras especializadas que ofrecen servicios a otros dispositivos en la red (clientes).

Ejecutan un **Network Operating System (NOS)** y suelen estar dedicadas a funciones específicas.

Tipos de servidores más comunes:

- **File Server:** almacena y distribuye archivos.
- **Mail Server:** gestiona el correo electrónico.
- **Print Server:** controla las impresoras de red.

- **Web Server:** aloja páginas web y contenido HTTPS.
- **Application Server:** ejecuta aplicaciones de red.
- **Proxy Server:** actúa en nombre de otros dispositivos para filtrar o redirigir tráfico.
- **Telephony Server:** gestiona llamadas y comunicaciones VoIP.



Nota: Los servidores deben ubicarse en áreas seguras, ya que almacenan información crítica y requieren alta disponibilidad.

◆ **Hosts**

Cualquier dispositivo que posea una dirección IP y pueda comunicarse dentro de la red.

En el contexto TCP/IP, un *host* puede ser un **servidor, una workstation, o cualquier otro dispositivo de red** con dirección IP asignada.

Ejemplo: en una red corporativa, tanto un servidor web como un portátil de un empleado son considerados *hosts*.

6. Tipos de redes

Las redes se clasifican según su alcance y propósito. A continuación, se describen las más comunes:

- ◆ **PAN (Personal Area Network)**

Red de corto alcance, utilizada para conectar dispositivos personales (como smartphones, portátiles o periféricos). Puede usar tecnologías **Bluetooth, infrared o ZigBee**.

Ejemplo: compartir conexión entre un teléfono móvil y un portátil mediante *tethering*.

- ◆ **LAN (Local Area Network)**

Red local de ámbito limitado (hogar, oficina o planta). Ofrece alta velocidad y baja latencia.

- ◆ **CAN (Campus Area Network)**

Conecta varias LAN dentro de un mismo campus corporativo o universitario.

Se encuentra entre la LAN y la MAN en cuanto a tamaño y alcance.

- ◆ **MAN (Metropolitan Area Network)**

Red metropolitana que conecta varios edificios o sedes dentro de una misma ciudad, generalmente a través de un proveedor de servicios (carrier).

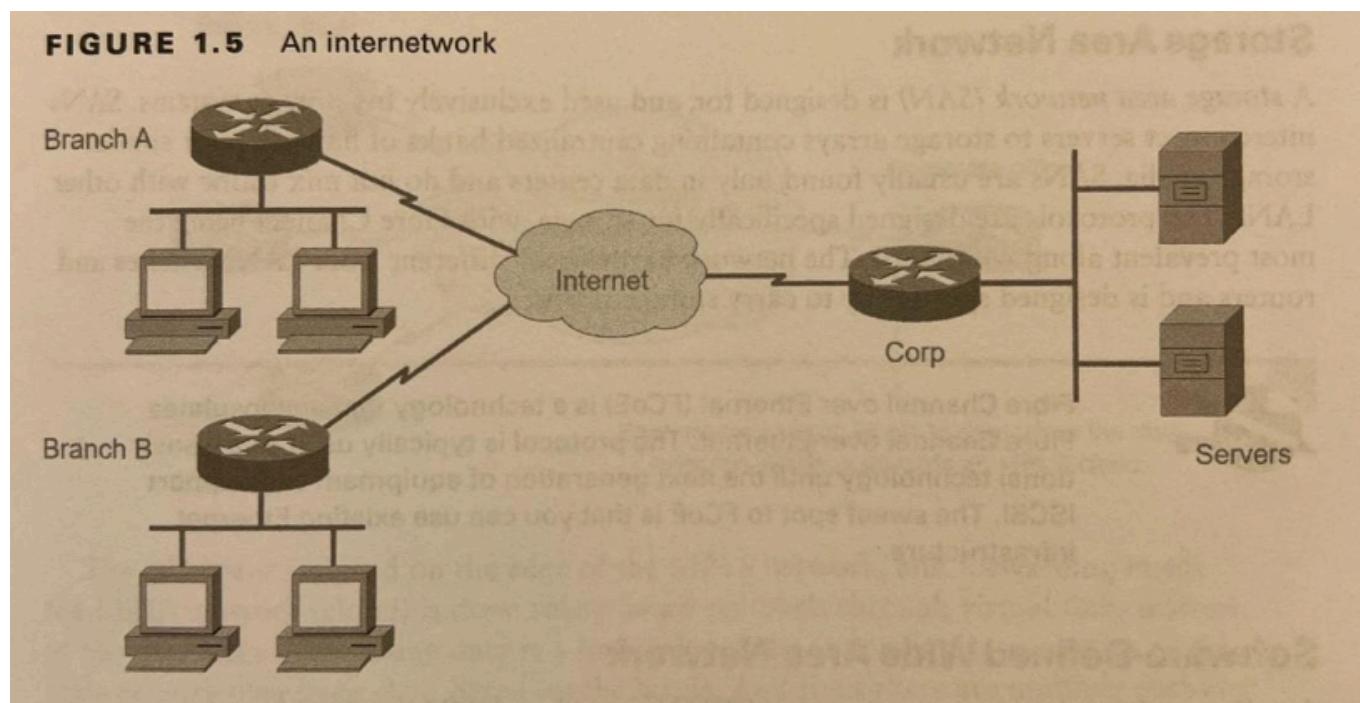
Utiliza enlaces de fibra óptica de alta velocidad.

◆ WAN (Wide Area Network)

Conecta redes a gran escala geográfica (por ejemplo, sedes en distintas ciudades o países). Utiliza **routers** y enlaces públicos o privados.

Características clave:

- Requiere **puertos de router** y enlaces dedicados. (router port or ports)
- Es más **lenta** que una LAN.
- Permite **enlaces entre redes distantes**.



Ejemplo: Internet es la WAN más grande del mundo.

◆ **SAN (Storage Area Network)**

Diseñada exclusivamente para el tráfico de almacenamiento. Interconecta servidores con cabinas de discos o sistemas de respaldo. Utiliza protocolos como **iSCSI** o **Fibre Channel**.

Permite gran ancho de banda y redundancia para almacenamiento masivo.

◆ **SDWAN (Software-Defined Wide Area Network)**

Arquitectura WAN virtual que usa software para gestionar conexiones, dispositivos y servicios.

Ventajas:

- Flexibilidad para redirigir tráfico o agregar ancho de banda.
- Reducción de costes y complejidad.
- Mayor visibilidad y control sobre el tráfico.

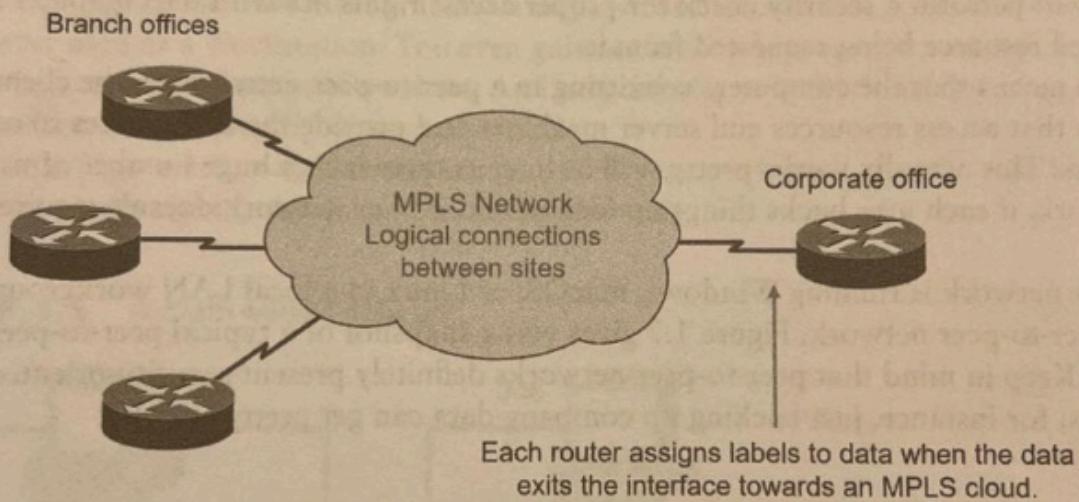
◆ **MPLS (Multiprotocol Label Switching)**

Tecnología WAN que usa **etiquetas (labels)** para enrutar datos en lugar de direcciones IP.

Ventajas principales:

- Flexibilidad en el diseño físico.
- Priorización de tráfico (por ejemplo, voz sobre datos).
- Redundancia en caso de fallo.
- Conectividad *one-to-many* (una sede a múltiples destinos).

FIGURE 1.6 Multiprotocol Label Switching layout



The labels are assigned on the edge of the MPLS network, and forwarding inside the MPLS network (cloud) is done solely based on labels through virtual links instead of physical links. Prioritizing data is a huge advantage; for example, voice data could have priority over basic data based on the labels. And since there are multiple paths for the data to be forwarded through the MPLS cloud, there's even some redundancy provided as well.

7. mGRE (Multipoint Generic Routing Encapsulation)

El protocolo **mGRE** permite la creación de túneles VPN dinámicos entre múltiples nodos sin necesidad de configurarlos manualmente. Es ampliamente utilizado en **Dynamic Multipoint VPN (DMVPN)**, donde los túneles se crean y destruyen según sea necesario.

8. Network Architectures

Una **network architecture** describe cómo se organizan los dispositivos dentro de una red y cómo se comunican entre ellos. Existen dos arquitecturas principales:

- ◆ **Peer-to-Peer (P2P)**

En una arquitectura **peer-to-peer**, todos los equipos de la red tienen la misma jerarquía y pueden **compartir recursos directamente entre sí**, sin depender de un servidor central.

Características principales:

- No hay control centralizado.
- Cada *peer* puede actuar como cliente o servidor según sea necesario.
- Configuración sencilla y económica.
- No requiere un *Network Operating System* dedicado.
- Adecuado para redes pequeñas (por ejemplo, hogares o pequeñas oficinas).

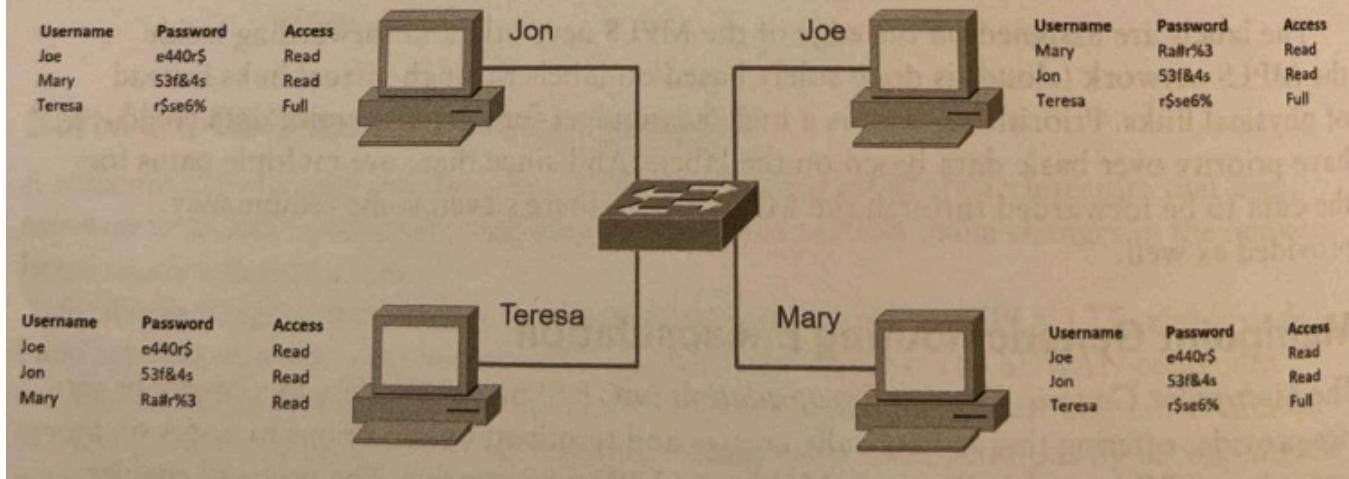
Peer-to-Peer Networks

Computers connected in *peer-to-peer networks* do not have any central or special authority—they’re all *peers*, meaning that when it comes to authority, they’re all equals. The authority to perform a security check for proper access rights lies with the computer that has the desired resource being requested from it.

It also means that the computers coexisting in a peer-to-peer network can be client machines that access resources and server machines and provide those resources to other computers. This actually works pretty well as long as there isn’t a huge number of users on the network, if each user backs things up locally, and if your network doesn’t require much security.

If your network is running Windows, macOS, or Linux in a local LAN workgroup, you have a peer-to-peer network. Figure 1.7 gives you a snapshot of a typical peer-to-peer network. Keep in mind that peer-to-peer networks definitely present security-oriented challenges; for instance, just backing up company data can get pretty sketchy!

FIGURE 1.7 A peer-to-peer network



Ejemplo:

Un grupo de cinco ordenadores conectados por un *switch*, compartiendo archivos y una impresora, sin dominio ni servidor dedicado.

Ventajas:

- Simplicidad y bajo coste.

- Menor mantenimiento.
- Ideal para entornos domésticos o de prueba.

Desventajas:

- Falta de control de acceso centralizado.
- Seguridad limitada.
- Dificultad para gestionar gran número de usuarios.
- Sin administración central de backups o permisos.

◆ Client/Server

En una arquitectura **client/server**, un dispositivo central (*server*) proporciona servicios o recursos a múltiples clientes dentro de la red.

Características:

- Los *servers* ejecutan un **Network Operating System (NOS)**, como *Windows Server* o *Linux*.

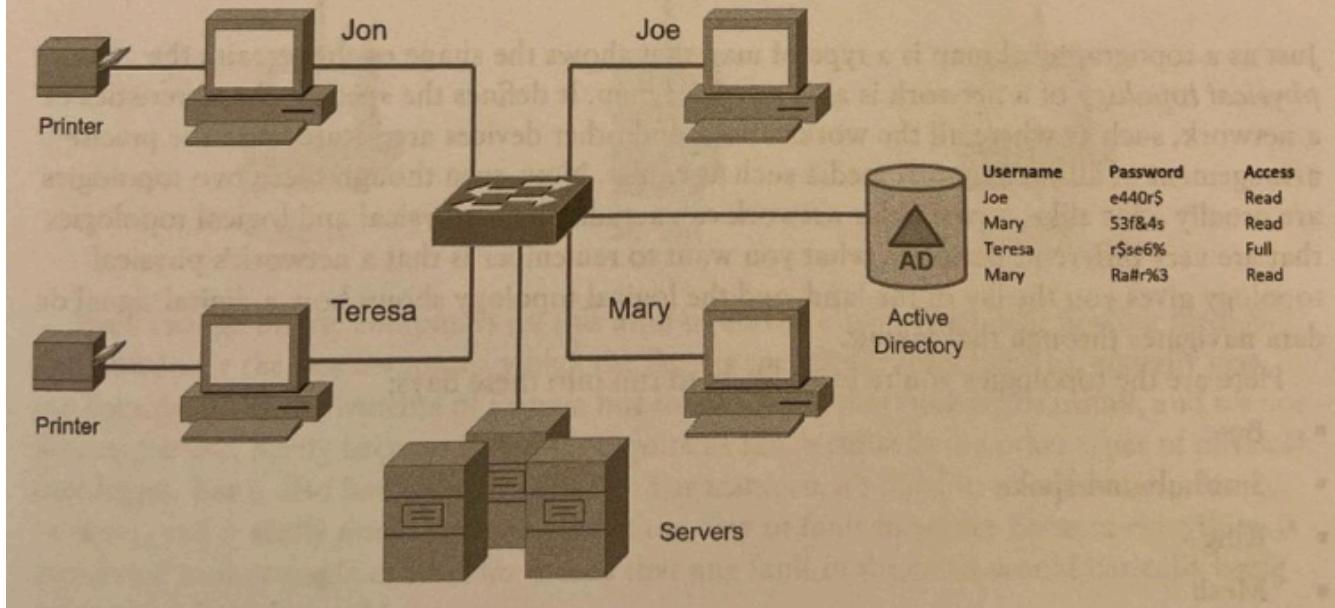
- Los *clients* dependen del servidor para autenticarse, acceder a archivos, impresoras, aplicaciones o bases de datos.
- Control centralizado sobre la seguridad y los permisos.
- Escalable y adecuado para redes medianas o grandes.

Client-Server Networks

Client-server networks are pretty much the polar opposite of peer-to-peer networks because in them, a single server uses a network operating system for managing the whole network. Here's how it works: A client machine's request for a resource goes to the main server, which responds by handling security and directing the client to the desired resource. This happens instead of the request going directly to the machine with the desired resource, and it has some serious advantages. First, because the network is much better organized and doesn't depend on users remembering where needed resources are, it's a whole lot easier to find the files you need because everything is stored in one spot—on that specific server. Your security also gets a lot tighter because all usernames and passwords are on that specific server, which is never ever used as a workstation. You even gain scalability because client-server networks can have legions of workstations on them. And surprisingly, with all those demands, the network's performance is actually optimized—nice!

Check out Figure 1.8, which shows a client-server network with a server that has a database of access rights, user accounts, and passwords.

FIGURE 1.8 A client-server network



Ejemplo:

Un servidor de archivos en una red corporativa almacena documentos para los usuarios, que acceden mediante sus credenciales personales.

Ventajas:

- Mayor seguridad y control administrativo.
- Facilita la gestión de usuarios y grupos.
- Posibilidad de aplicar políticas (*Group Policy Objects*, ACLs).
- Mejora el rendimiento mediante servidores dedicados a funciones específicas.

Desventajas:

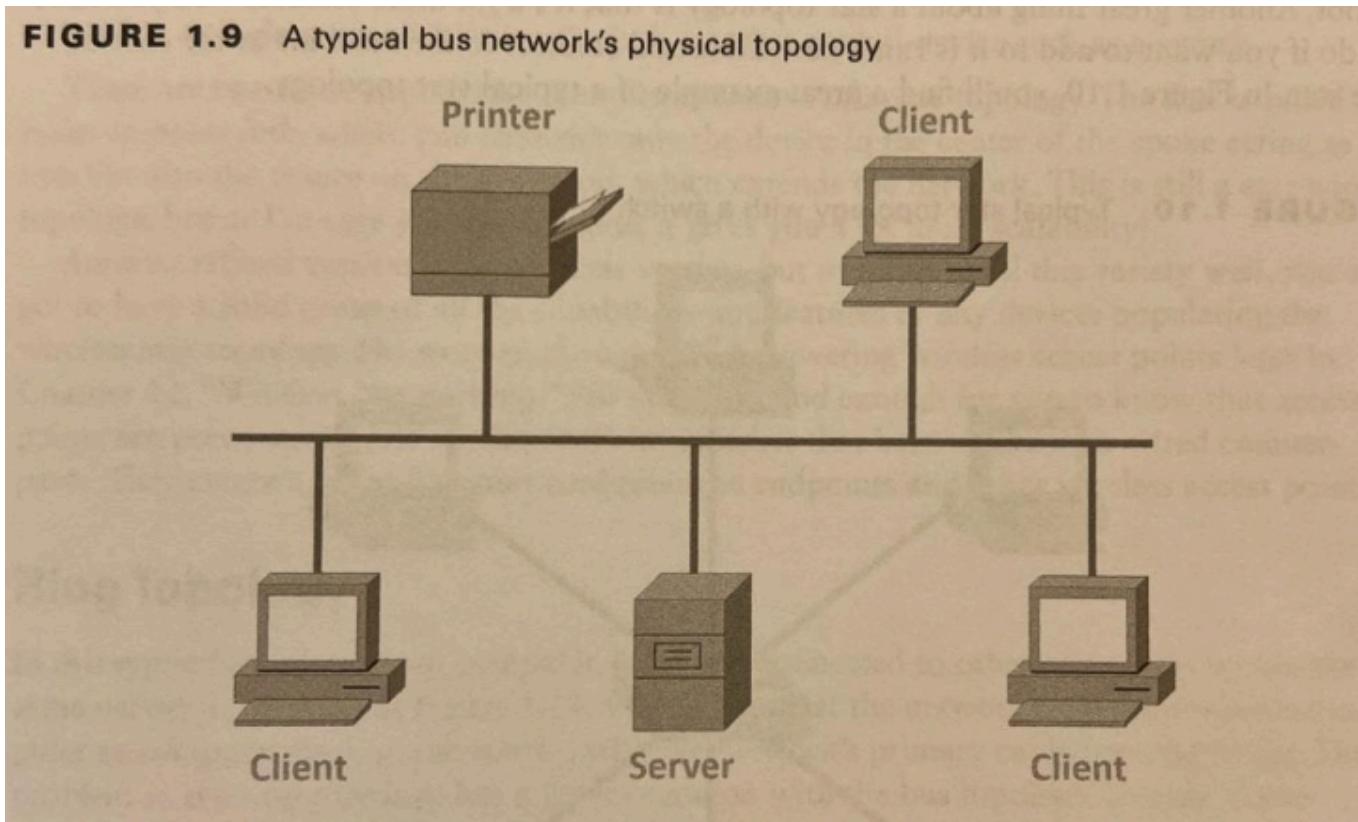
- Mayor coste de instalación y mantenimiento.
 - Requiere hardware y software especializados.
 - Dependencia del servidor: si falla, el servicio se interrumpe.
-

9. Physical Topologies

La **topología física (physical topology)** describe la forma en que los dispositivos están físicamente conectados en la red. Aunque el tráfico lógico pueda diferir, la estructura física determina el rendimiento, la redundancia y la facilidad de administración.

◆ Bus Topology

En una **bus topology**, todos los dispositivos comparten un único cable central (*backbone cable*) que transporta los datos.



Características:

- Solo un canal de comunicación.
- Cada nodo escucha el tráfico y responde si le corresponde.
- Si el cable principal falla, toda la red se cae.

Ventajas:

- Bajo coste.
- Sencilla de implementar.
- Ideal para redes pequeñas o de laboratorio.

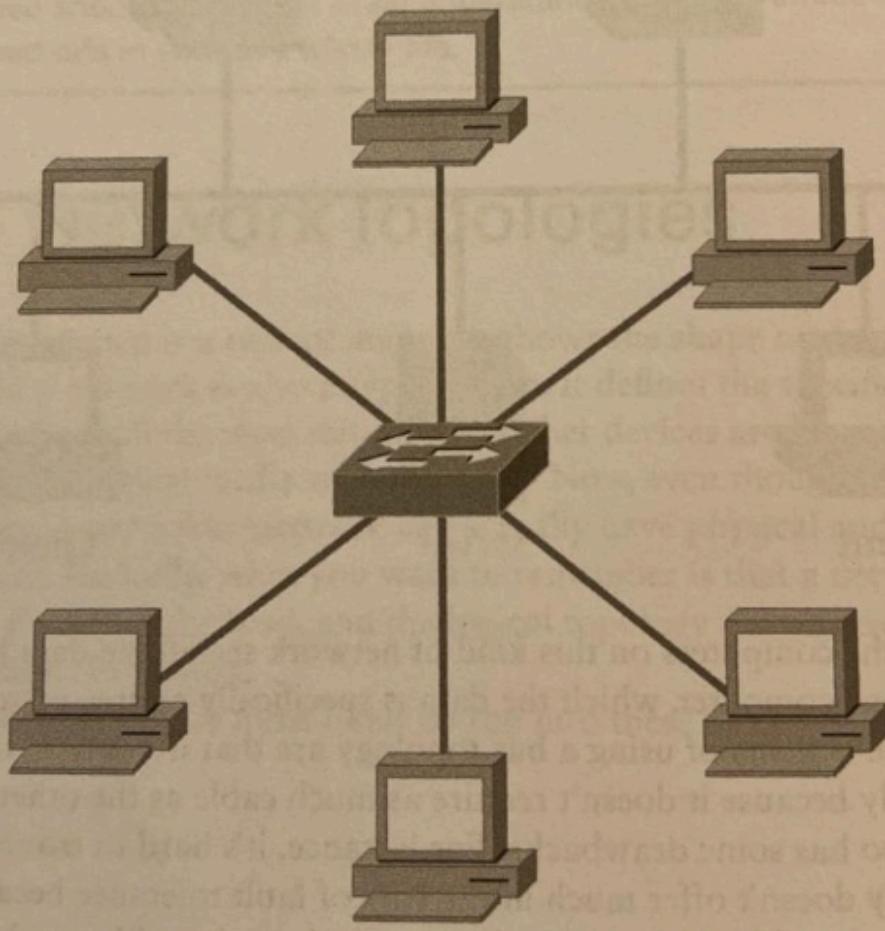
Desventajas:

- Dificultad para aislar fallos.
- Baja escalabilidad.
- Colisiones de tráfico frecuentes.
- Obsoleta en la mayoría de entornos modernos.

◆ **Star Topology**

La **star topology** conecta cada dispositivo a un punto central (normalmente un *switch* o *hub*). Es el diseño más común en redes modernas.

FIGURE 1.10 Typical star topology with a switch



Características:

- Cada conexión es independiente.
- Si un cable individual falla, solo afecta al dispositivo correspondiente.
- El nodo central es crítico: si falla, toda la red cae.

Ventajas:

- Alta fiabilidad y facilidad de mantenimiento.

- Fácil detección de fallos.
- Escalable y compatible con velocidades modernas (1 Gbps o más).
- Ideal para *Ethernet LANs*.

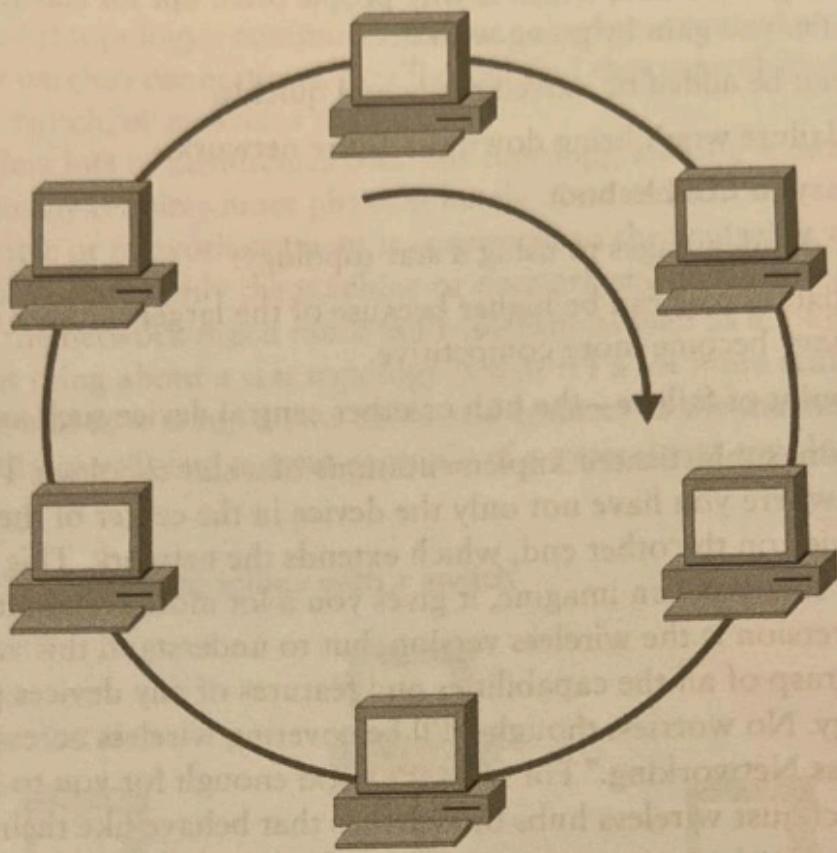
Desventajas:

- Dependencia del punto central.
 - Mayor coste de cableado.
-

◆ **Ring Topology**

En una **ring topology**, cada dispositivo está conectado al siguiente formando un bucle cerrado.

FIGURE 1.11 A typical ring topology



Características:

- Los datos viajan en una única dirección (*unidirectional*).
- Cada nodo actúa como repetidor, regenerando la señal.
- Un fallo en un nodo puede interrumpir el anillo completo.

Ventajas:

- Rendimiento predecible.
- No se producen colisiones.
- Adecuada para redes con tráfico uniforme.

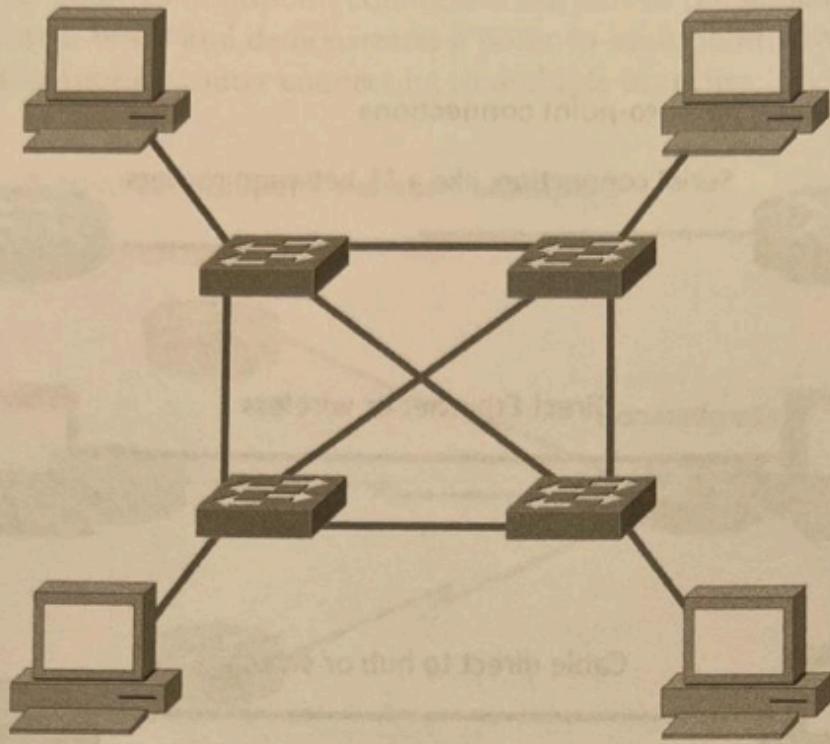
Desventajas:

- Difícil de configurar y mantener.
 - Baja tolerancia a fallos.
 - Obsoleta frente a las topologías modernas (como *star* o *mesh*).
-

◆ **Mesh Topology**

En una **mesh topology**, cada nodo está conectado directamente con varios (o todos) los demás.

FIGURE 1.12 A typical mesh topology



Tipos:

- **Full Mesh:** todos los dispositivos están interconectados.
- **Partial Mesh:** algunos dispositivos tienen enlaces redundantes.

Ventajas:

- Alta redundancia y disponibilidad.
- Rutas múltiples para el tráfico (ideal para entornos críticos).

- Se usa comúnmente en *WANs* y *wireless networks*.

Desventajas:

- Coste elevado de implementación.
 - Complejidad en la gestión y el cableado.
-

◆ **Point-to-Point Topology**

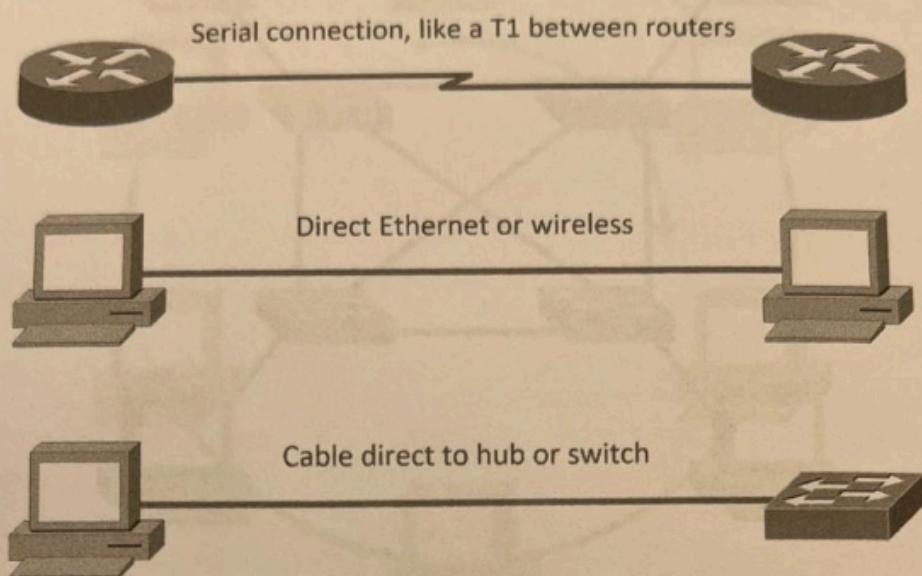
La **topología punto a punto (Point-to-Point)** establece una conexión directa entre dos dispositivos de red, como routers o switches, proporcionando una única ruta de comunicación. Es una configuración simple que puede realizarse mediante cableado físico (por ejemplo, una conexión serial) o mediante enlaces inalámbricos cuando los equipos están separados por cierta distancia.

Este tipo de topología se utiliza habitualmente en **redes WAN**, donde un enlace dedicado conecta dos ubicaciones concretas.

Aunque su implementación es sencilla y confiable, presenta una limitación importante: **no es escalable**. Cada nueva conexión requiere un enlace adicional independiente.

Figure 1.13 illustrates three examples of a typical T1, or WAN, point-to-point connection.

FIGURE 1.13 Three point-to-point connections



What you see here is a lightning bolt and a couple of round things with a bunch of arrows projecting from them, right? Well, the two round things radiating arrows represent our network's two routers, and that lightning bolt represents a WAN link. These symbols are industry standard, and I'll be using them throughout this book, so it's a good idea to get used to them!

So, the second part of the diagram shows two computers connected by a cable—a point-to-point link. By the way, this should remind you of something we just went over. Remember peer-to-peer networks? Good! I hope you also remember that a big drawback to peer-to-peer network sharing is that it's not very scalable. With this in mind, you probably won't be all that surprised that even if both machines have a wireless point-to-point connection, this network still won't be very scalable.

You'll usually find point-to-point networks within many of today's WANs, and as you can see in the third part of Figure 1.13, a link from a computer to a hub or switch is also a valid point-to-point connection. A common version of this setup consists of a direct wireless link between two wireless bridges that's used to connect computers in two different buildings together.



Podemos observar que esta estructura recuerda al modelo peer-to-peer, pero aplicado a nivel de red física.

Ejemplo de configuraciones Point-to-Point:

- Conexión serial (T1/E1) entre routers.
- Enlace Ethernet directo entre dos equipos.
- Conexión inalámbrica directa (bridge) entre dos edificios.

◆ **Point-to-Multipoint Topology**

La **topología punto a multipunto (Point-to-Multipoint)** extiende el concepto anterior, permitiendo que una interfaz (por ejemplo, un router corporativo) se comunique con múltiples destinos.

En este esquema, **un único punto central** conecta con varios nodos remotos o sucursales, siendo ideal para entornos WAN corporativos.

connection to multiple points of connection. Each of the routers and every one of their interfaces involved in the point-to-multipoint connection are part of the same network.

Figure 1.14 shows a WAN and demonstrates a point-to-multipoint network. You can clearly see a single, corporate router connecting to multiple branches.

FIGURE 1.14 A point-to-multipoint network, example 1

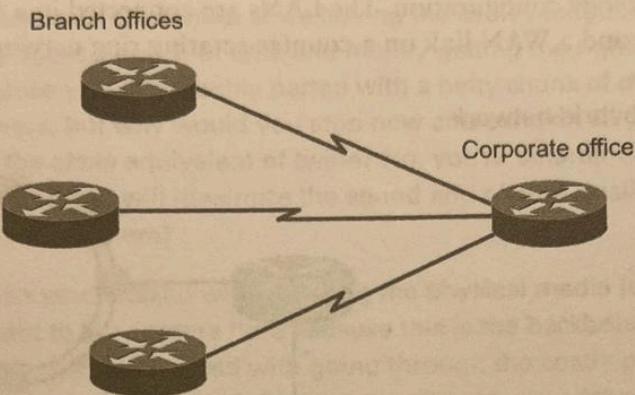
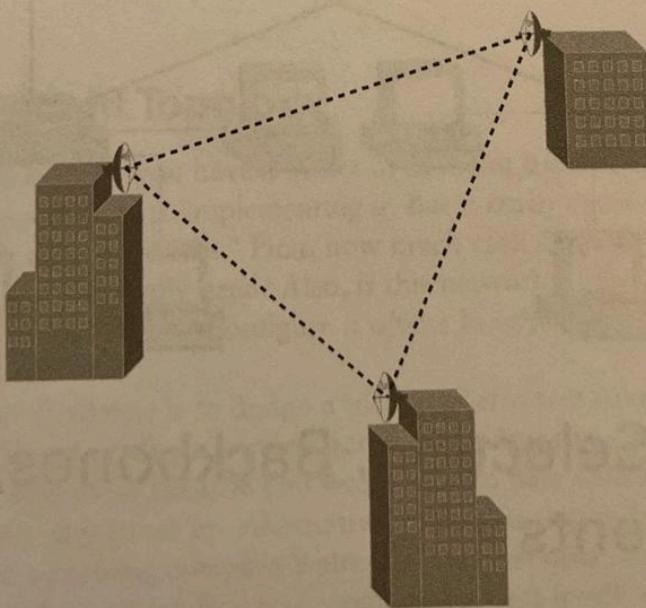


Figure 1.15 shows another prime example of a point-to-multipoint network: a college or corporate campus.

FIGURE 1.15 A point-to-multipoint network, example 2



Ventajas principales:

- Reducción de costes frente a enlaces dedicados múltiples.
- Mayor flexibilidad para ampliar o reconfigurar la red.
- Facilita la comunicación entre sede central y oficinas remotas.

Ejemplos prácticos:

- Un router corporativo conectando varias oficinas a través de enlaces WAN.
- Comunicaciones inalámbricas entre edificios de un campus (Figura 1.15).



En resumen, la topología point-to-multipoint combina eficiencia con escalabilidad, pero requiere una gestión cuidadosa del ancho de banda en el nodo central.

◆ Hybrid Topology

Una **hybrid topology** combina dos o más topologías físicas para aprovechar sus ventajas.

Ejemplos comunes:

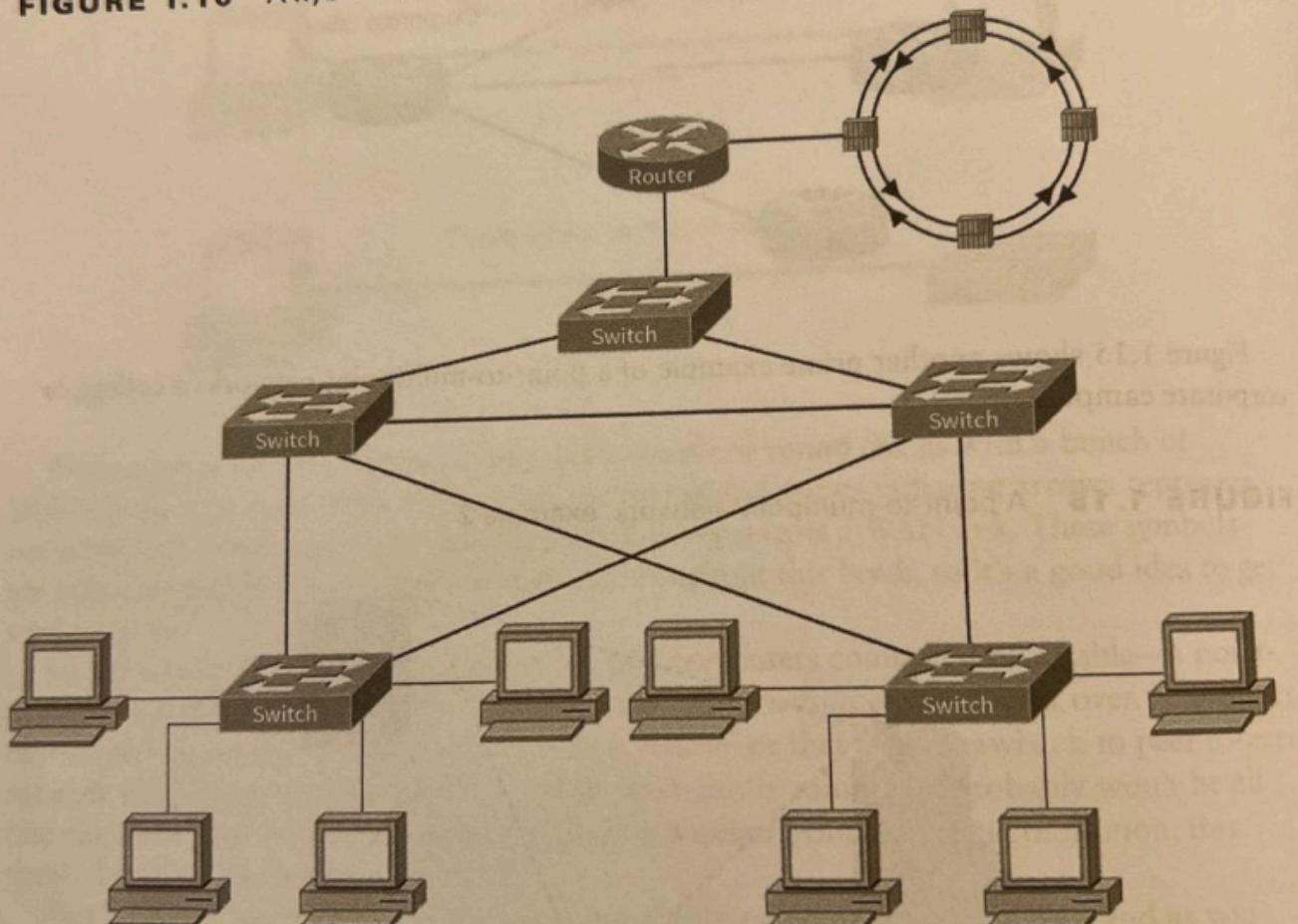
- **Star-Bus:** varias *star networks* interconectadas mediante un backbone.
- **Star-Ring:** varias *rings* conectadas a un concentrador central.

Hybrid Topology

I know I just talked about the hybrid network topology in the section about mesh topology, but I didn't give you a mental picture of it in the form of a figure. I also want to point out that *hybrid topology* means just that—a combination of two or more types of physical or logical network topologies working together within the same network.

Figure 1.16 depicts a hybrid network topology; it shows a few LANs connected by switches in a star topology configuration. The LANs are connected in a full mesh, which is connected to a router and a WAN link on a counter-rotating ring network.

FIGURE 1.16 A hybrid network





Ejemplo real:

Una gran universidad puede tener topologías *star* en cada edificio, conectadas entre sí mediante un *bus* o *backbone* de fibra óptica.

Ventajas:

- Flexible y adaptable.
- Escalable según las necesidades del entorno.

Desventajas:

- Coste y complejidad mayores.
- Difícil diagnóstico de fallos.

10. Logical vs Physical Topology

Es fundamental distinguir entre **topología física** y **topología lógica**, ya que ambas describen perspectivas diferentes de una misma red:

Tipo	Descripción	Ejemplo
Physical topology	<p>Describe cómo están dispuestos físicamente los dispositivos (hosts, switches, routers) y los medios de transmisión (cables, fibra, enlaces inalámbricos). Define la estructura visible de la red.</p>	<p>Una red con varios switches conectados por cables Ethernet formando una estrella.</p>
Logical topology	<p>Representa cómo fluyen los datos entre los dispositivos dentro de la red, independientemente de su disposición física. Determina la ruta lógica de comunicación y los protocolos implicados.</p>	<p>Una red <i>Ethernet</i> donde el tráfico sigue un patrón lógico de bus aunque físicamente esté conectada en estrella.</p>

 La **topología física** puede entenderse como el “mapa del cableado”, mientras que la **topología lógica** muestra “por dónde viaja la información”.

En muchos entornos empresariales, estas dos perspectivas no coinciden.

Por ejemplo, una red LAN moderna con switches utiliza una **configuración física en estrella**, pero los paquetes Ethernet se transmiten siguiendo un **esquema lógico de bus**, ya que los dispositivos comparten un mismo dominio de broadcast controlado por el switch.

Además, con la virtualización y las VLANs, la topología lógica puede **dividir o superponer redes** sobre una misma infraestructura física. Esto significa que una única red física puede albergar múltiples topologías lógicas simultáneamente, según la segmentación y las políticas de tráfico aplicadas.

En resumen, la **topología física define la estructura tangible** del cableado y hardware, mientras que la **topología lógica define la forma en que los dispositivos se comunican**, gestionan el tráfico y segmentan los dominios de red.

11. Hierarchical Network Model

El **modelo jerárquico de red (Hierarchical Network Model)** es un enfoque de diseño que divide la infraestructura en **capas funcionales** para facilitar la administración, la escalabilidad y la redundancia.

◆ Estructura del modelo

Capa	Función principal	Dispositivos típicos
Core Layer	Actúa como el backbone de la	Core switches,

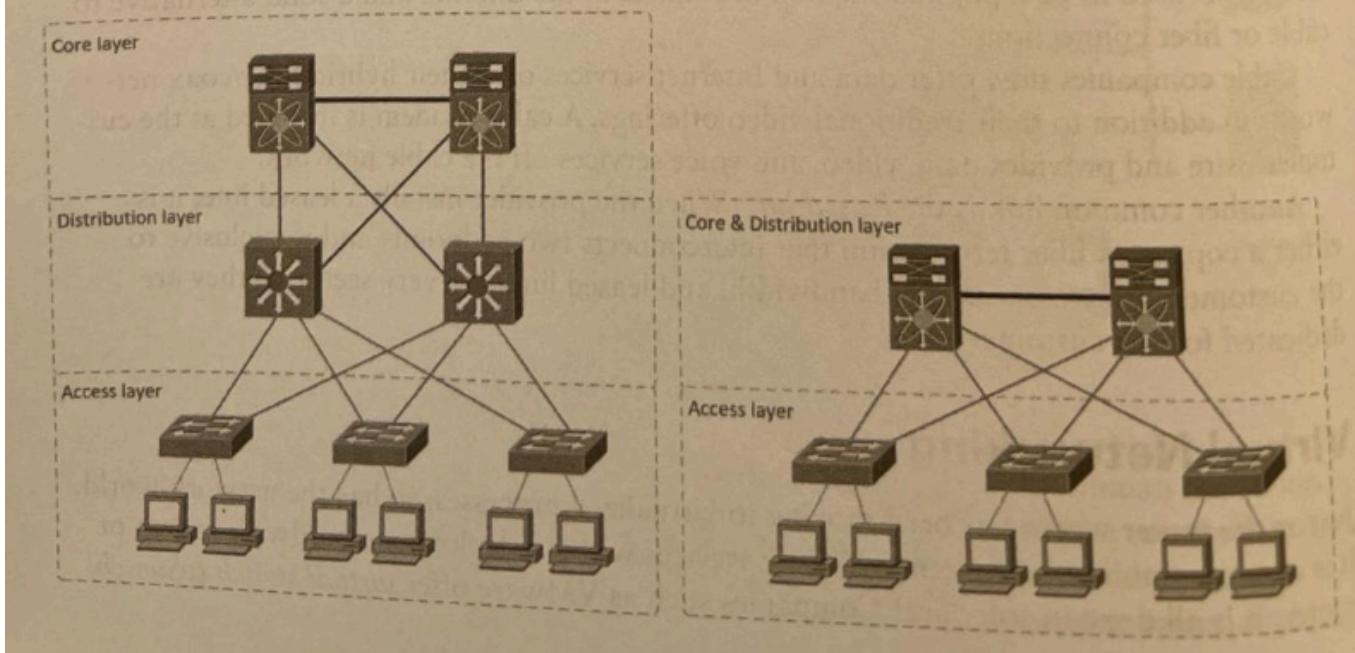
Capa	Función principal	Dispositivos típicos
	red. Transporta grandes volúmenes de datos a alta velocidad entre routers o switches principales.	routers de alto rendimiento.
Distribution Layer	Gestiona el enrutamiento entre VLANs , aplica políticas de seguridad, filtrado y control de acceso.	Switches de capa 3, firewalls, routers.
Access Layer	Conecta los hosts y dispositivos finales , proporcionando acceso a los recursos de red.	Switches de acceso, puntos de acceso Wi-Fi.

■ Este modelo, también conocido como **Cisco Hierarchical Design Model**, se basa en la modularidad. Cada capa puede ampliarse o modificarse sin alterar las demás.

Three-Tiered Model

The three-tiered networking model was introduced more than 20 years ago by Cisco, and it's been the gold-standard for network design. Even though it was introduced so long ago, it is still very much valid today for any hardware vendor. However, in today's small to midsize network designs, the collapsed-core model has been adopted to save the expense of additional network switching, as shown in Figure 1.18. The elements of both models are similar in function.

FIGURE 1.18 Three-tier versus collapsed-core model



- ◆ **Ventajas del modelo jerárquico**
 - Escalabilidad: permite crecimiento estructurado de la red.

- Redundancia: soporta múltiples caminos de datos.
- Seguridad: segmenta las funciones y políticas.
- Administración más sencilla: cada capa tiene un propósito claro.



Ejemplo:

En una organización, la capa de acceso conecta los equipos de los empleados, la de distribución enruta entre departamentos, y la capa core interconecta los edificios principales o data centers.

12. Network Backbone

El **backbone**, también conocido como *core network*, es la **columna vertebral de la infraestructura**. Su función es **interconectar los distintos segmentos o subredes** y transportar el tráfico de red de manera eficiente.

- ◆ **Características principales**

- Alta capacidad de transmisión (Gigabit o superior).
- Implementación con **fibra óptica** para minimizar la latencia.
- Enlaces redundantes para aumentar disponibilidad.
- Conecta switches, routers y firewalls de nivel superior.

◆ **Tipos de backbone**

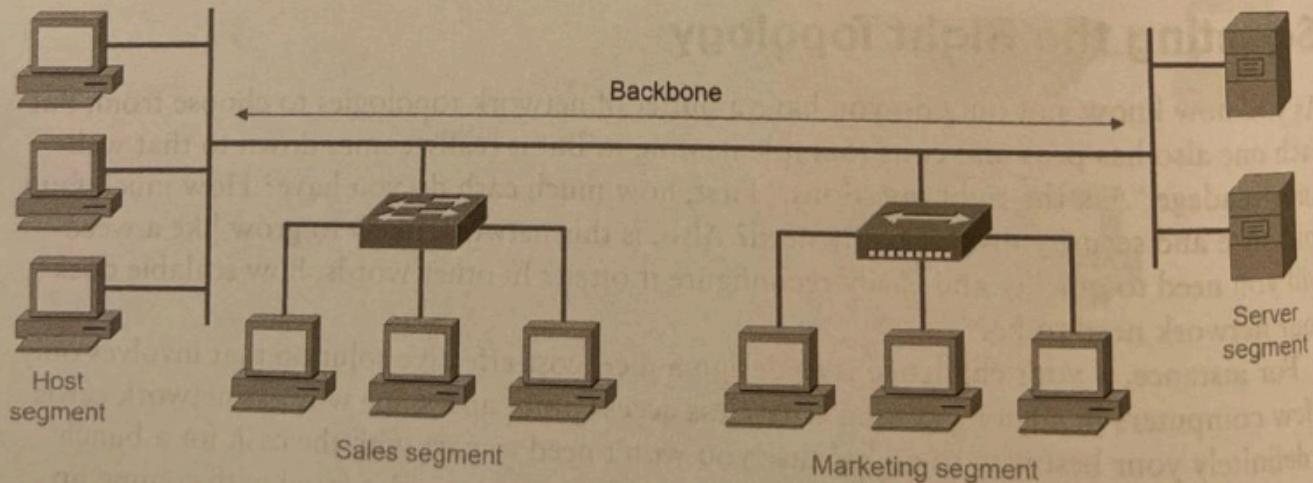
- **Collapsed Backbone:** concentración de toda la red en un switch o router central.
- **Distributed Backbone:** múltiples dispositivos de interconexión organizados por capas (típico del modelo jerárquico).
- **Parallel Backbone:** enlaces duplicados entre nodos principales para redundancia.
- **Core-Distribution Backbone:** diseño mixto con switches de núcleo y distribución conectados por enlaces de fibra dedicados.

The Network Backbone

Today's networks can get pretty complicated, so we need to have a standard way of communicating with each other intelligibly about exactly which part of the network we're referencing. This is the reason we divide networks into different parts called *backbones* and *segments*.

Figure 1.17 illustrates a network and shows which part is the backbone and which parts are segments.

FIGURE 1.17 Backbone and segments on a network



You can see that the network backbone is actually kind of like our own human backbone. It's what all the network segments and servers connect to and what gives the network its structure. As you can imagine, being such an important nerve center, the backbone must use some kind of seriously fast, robust technology—often Gigabit Ethernet or faster. And to



Ejemplo:

Un campus universitario puede tener backbones de fibra entre edificios, cada uno con su propia LAN local.

Ventajas:

- Incrementa el rendimiento general.

- Facilita el control del tráfico.
 - Mejora la resiliencia ante fallos de enlace.
-

13. Network Segments

El término **network segment** hace referencia a cualquier porción de una red que, aunque conectada al backbone, funciona de forma lógica o física como una sección independiente.

Cada segmento contiene estaciones de trabajo y servidores que se comunican localmente antes de pasar al backbone.

Beneficios:

- Reducción del tráfico broadcast.
- Mejora del rendimiento y eficiencia.
- Facilita la administración y la seguridad al aislar grupos funcionales.



Ejemplo: los departamentos de Ventas, Finanzas y Soporte pueden considerarse tres

segmentos distintos dentro de una misma red corporativa.

14. Service-Related Entry Points

En redes empresariales, existen puntos específicos donde una red interna se enlaza con la infraestructura de un **proveedor de servicios (carrier)**. Estos puntos se denominan **Service-Related Entry Points** y marcan el límite de responsabilidad entre el cliente y el proveedor.

- **Demarcation point (demarc)**: punto físico donde termina la red del proveedor y comienza la del cliente.
- **Smart jack**: dispositivo instalado por el carrier que permite diagnóstico remoto y verificación de señal hasta el punto de entrega.

 En otras palabras, el demarc determina quién es responsable ante una avería, y el smart

jack ofrece una interfaz segura para pruebas sin afectar la red del cliente.

15. Service Provider Links

Los **Service Providers** (ISP, compañías telefónicas, operadoras de cable) ofrecen distintas tecnologías para enlazar la red del cliente con Internet o con otras sedes.

Entre los métodos más comunes se encuentran:

- **DSL (Digital Subscriber Line)**: conexión sobre par de cobre. Aún usada en entornos residenciales o pymes.
- **Cable Modem (HFC)**: tecnología híbrida fibra-coaxial que permite datos, voz y vídeo.
- **Leased Line**: línea dedicada punto a punto con ancho de banda reservado y alta seguridad.
- **Satellite Link**: opción para ubicaciones remotas sin infraestructura terrestre.



Nota: las **leased lines** son altamente fiables ya que el ancho de banda no se comparte con otros clientes, lo que garantiza una conexión estable y privada.

16. Spine-Leaf Architecture

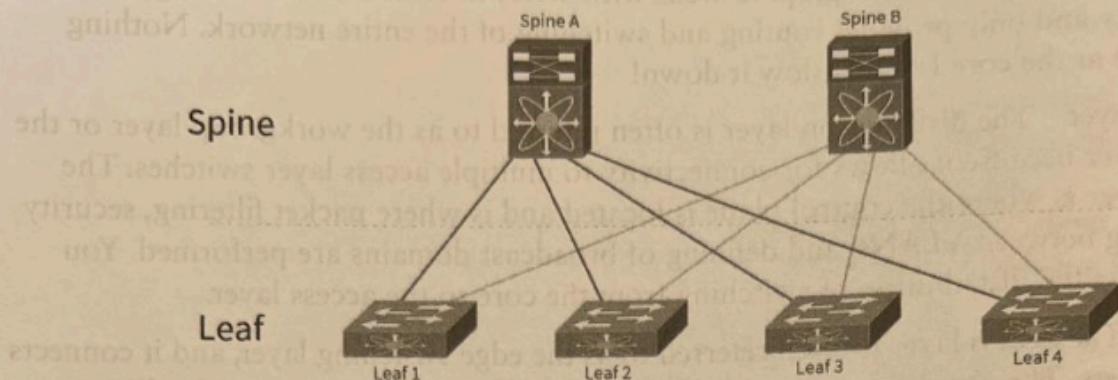
La **spine-leaf topology** es una **evolución moderna del modelo jerárquico tradicional**, ampliamente utilizada en centros de datos (*data centers*).

El objetivo es optimizar el flujo de tráfico **este-oeste (east-west)** entre servidores virtualizados.

◆ Estructura

- Los **spine switches** forman el **core** de la red.
- Los **leaf switches** se conectan a los dispositivos finales (servidores, VMs, storage).
- Cada *leaf* se conecta con **todos los spines**, eliminando cuellos de botella.

FIGURE 1.19 A typical spine-leaf network



As you can see in Figure 1.19, the Spine A switch is connected to every leaf switch, and the Spine B switch is connected to every leaf switch. This allows extremely fast switching between Leaf 1 and Leaf 4 as well as any other leaf switch. Switching between two leaf switches is always two hops away no matter where they are in the network. It will traverse to the spine switch and then to the destination leaf switch.

Ventajas:

- Alta redundancia y disponibilidad.
- Latencia predecible y baja.
- Rutas múltiples sin bucles (*loop-free design*).
- Escalabilidad horizontal: pueden añadirse más *leafs* sin rediseñar.

Desventajas:

- Coste inicial mayor.
- Complejidad de configuración.



En una arquitectura jerárquica clásica, el tráfico suele moverse “norte-sur”. En cambio, en un diseño *spine-leaf* el tráfico es predominantemente “este-oeste”, ideal para entornos virtualizados con alto intercambio de datos entre servidores.

17. Virtualization in Networking

La **virtualización de red** permite crear entornos flexibles, definidos por software, en los que múltiples redes o servicios pueden coexistir en el mismo hardware físico.

- ◆ **Virtual Network Functions (VNF)**

Componentes tradicionales de red —como routers, firewalls o load balancers— ejecutados como software en lugar de dispositivos dedicados.

◆ Network Virtualization

Combinación de recursos físicos y virtuales para generar redes lógicas independientes.

Permite crear *overlay networks* que operan sobre una red física subyacente.



Tecnologías clave:

- **VLAN (Virtual LAN)**: segmentación lógica dentro de un switch físico.
- **VXLAN (Virtual Extensible LAN)**: extiende VLANs a redes distribuidas y virtualizadas.
- **SDN (Software-Defined Networking)**: controla de forma centralizada las redes físicas y virtuales.

Ventajas:

- Aislamiento entre entornos.
- Mayor aprovechamiento de recursos.
- Simplificación en pruebas y despliegues.

18. Software-Defined Networking (SDN)

El **Software-Defined Networking (SDN)** es un paradigma que separa el **control plane** (gestión de decisiones de tráfico) del **data plane** (encaminamiento real de los datos).

◆ Componentes principales

- **Controller:** cerebro de la red, define y envía reglas de enrutamiento.
- **Network Devices:** switches o routers programables que siguen las instrucciones del controlador.
- **Applications:** software que utiliza las APIs del controlador para automatizar tareas.

Ventajas:

- Centralización del control.
- Automatización y reconfiguración dinámica.
- Reducción de errores humanos.

- Integración con *cloud* y entornos virtualizados.

Desventajas:

- Complejidad inicial y curva de aprendizaje.
- Dependencia del controlador SDN.
- Riesgo de punto único de fallo si no hay redundancia.



Ejemplo práctico:

Un administrador puede modificar la priorización de tráfico (QoS) o crear nuevas VLANs desde una consola central, sin acceder físicamente a los switches.

19. Virtual Hosts and Network Segmentation

Los **virtual hosts** (VMs) se ejecutan sobre un *hypervisor* como VMware ESXi, Hyper-V o KVM, comportándose como hosts independientes con su propio sistema operativo y dirección IP.

◆ Características

- Se comunican a través de **switches virtuales (vSwitches)**.
- Pueden pertenecer a VLANs distintas.
- El tráfico puede ser interno (entre VMs) o externo (hacia la red física).

Ventajas:

- Aislamiento entre servicios.
- Ahorro de recursos físicos.
- Facilidad de copia y migración (*live migration*).



Ejemplo:

Un mismo servidor físico puede ejecutar una VM de *Web Server*, otra de *Database Server* y otra de *Testing Environment* dentro de la misma infraestructura.

20. Network Traffic Flow

El flujo de tráfico (traffic flow) describe cómo se mueven los paquetes a través de la red y cómo varía según el diseño o la arquitectura.

- ◆ **North-South Traffic**

Flujo **vertical** entre usuarios y servicios externos o centrales (como Internet o data centers).

| Ejemplo: un usuario accede a un servidor web.

- ◆ **East-West Traffic**

Flujo **horizontal** entre dispositivos dentro del mismo segmento o data center.

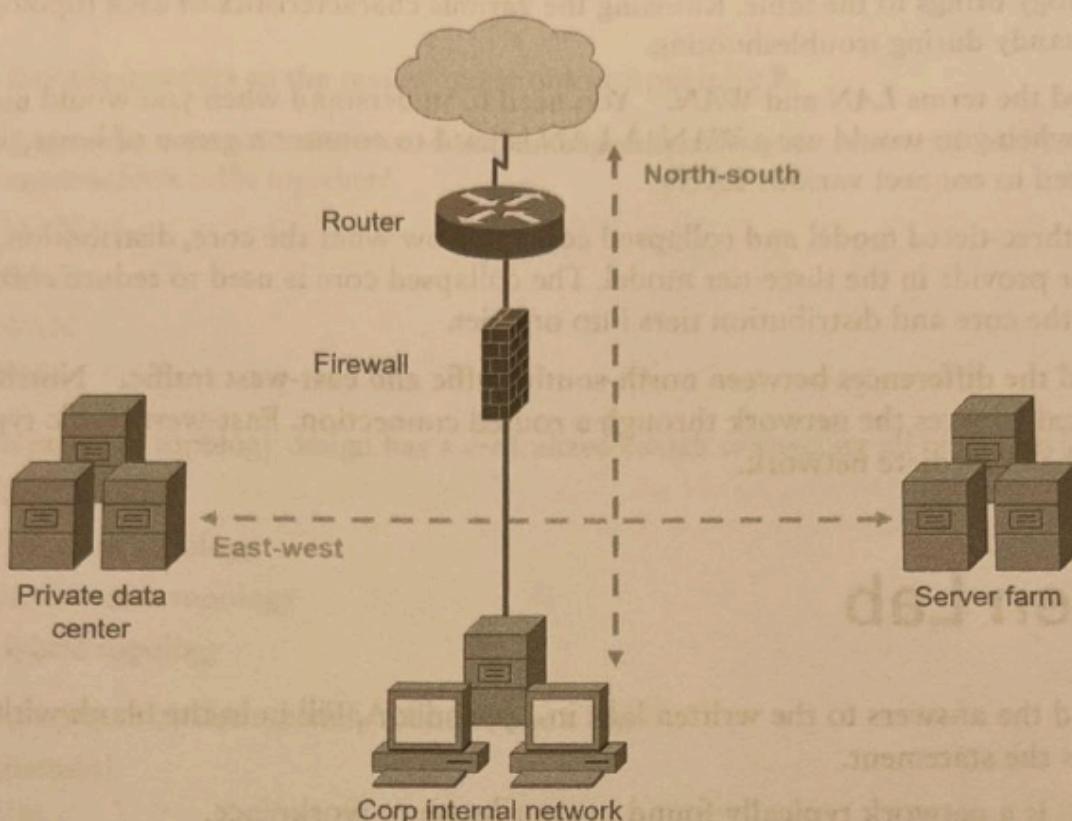
| Ejemplo: intercambio de datos entre servidores virtualizados.

- ◆ **Tipos de tráfico**

Tipo	Descripción	Ejemplo
Unicast	Comunicación uno-a-uno.	Un cliente descarga un

Tipo	Descripción	Ejemplo
		archivo de un servidor.
Multicast	Comunicación uno-a-muchos (solo suscritos).	Transmisión de vídeo a varias sucursales.
Broadcast	Comunicación uno-a-todos.	Petición ARP dentro de una LAN.

FIGURE 1.20 Understanding traffic flow in your network



 En redes extensas, el tráfico *broadcast* debe controlarse mediante segmentación o VLANs para evitar congestión.

21. Network Segmentation and Performance

La **segmentación de red** consiste en dividir una red en **subnets** o **VLANs** para controlar el tráfico y mejorar el rendimiento.

Beneficios:

- Menor congestión al reducir dominios de broadcast.
- Aumento de la seguridad al aislar departamentos.
- Mayor facilidad de diagnóstico y administración.
- Posibilidad de aplicar políticas por segmento.



Ejemplo práctico:

Dividir los departamentos de *Finanzas*, *IT* y *RRHH* en VLANs separadas con diferentes políticas de acceso.

22. Summary

Podemos observar que las redes modernas evolucionan hacia **infraestructuras modulares, virtualizadas y definidas por software**, donde el flujo de datos es flexible y la administración se centra en la eficiencia y seguridad.

En este capítulo hemos revisado:

- El **modelo jerárquico de red** y su relación con el backbone.
- La **arquitectura spine-leaf** como alternativa para centros de datos.
- Conceptos clave de **virtualización** y **SDN**.
- La importancia del **flujo de tráfico** (norte-sur y este-oeste).

- La **segmentación lógica y física** para optimizar rendimiento y control.

 Diferenciando de esta manera la infraestructura tradicional, centrada en dispositivos físicos, de las soluciones modernas orientadas a la automatización, la virtualización y la resiliencia.

23. Exam Essentials

- **Identifica los tipos de red.**
LAN, WAN, MAN, CAN y PAN son los más comunes; cada uno difiere por alcance y propósito.
- **Reconoce las arquitecturas de red.**
Peer-to-peer es simple pero limitada; *client/server* ofrece control y escalabilidad.
- **Comprende las topologías físicas.**
Star es la más usada actualmente; *mesh* se reserva para entornos críticos.

- **Distingue entre topología física y lógica.**
La física describe el cableado; la lógica, el flujo de datos.
 - **Aplica el modelo jerárquico y la spine-leaf topology.**
Son esenciales para el diseño escalable de redes corporativas.
 - **Conoce los fundamentos de SDN y virtualización.**
La red moderna se programa y gestiona mediante software.
-

24. Written Lab

Actividad:

Explica en tus propias palabras cómo se comportan los siguientes escenarios de red:

1. Diferencia el tráfico norte-sur del este-oeste en un entorno virtualizado.
2. Describe qué ventajas aporta una topología

spine-leaf frente a una jerárquica clásica.

3. Indica qué tipo de red (LAN, WAN, MAN, etc.) usarías para interconectar tres edificios de una misma empresa en la misma ciudad, justificando tu respuesta.



Objetivo: Aplicar conceptos teóricos del capítulo a situaciones prácticas.

25. Review Questions (traducción y explicación)



1. Which type of network connects devices within a single building or campus area?

¿Qué tipo de red conecta dispositivos dentro de un solo edificio o campus?

Opciones:

- A. MAN (Metropolitan Area Network)

- B. WAN (Wide Area Network)
- C. LAN (Local Area Network)
- D. CAN (Campus Area Network)

 **Respuesta correcta:** C. LAN (Local Area Network)

Explicación:

Una **LAN** cubre áreas geográficas pequeñas, como oficinas, plantas o campus reducidos. Ofrece alta velocidad y baja latencia. Las **MAN** y **WAN** abarcan distancias mucho mayores.

 **2. Which topology connects each device to a central point, such as a switch?**

¿Qué topología conecta cada dispositivo con un punto central, como un switch?

Opciones:

- A. Bus
- B. Mesh

C. Ring

D. Star

 **Respuesta correcta:** D. Star

Explicación:

En la **topología estrella**, todos los nodos se conectan a un switch o concentrador central. Si un cable falla, solo se ve afectado ese enlace, no toda la red.

 **3. In which type of architecture do computers communicate directly without a dedicated server?**

¿En qué tipo de arquitectura los ordenadores se comunican directamente sin un servidor dedicado?

Opciones:

A. Peer-to-Peer

B. Client/Server

- C. Hybrid
- D. Centralized

 **Respuesta correcta:** A. Peer-to-Peer

Explicación:

En la **arquitectura peer-to-peer**, todos los dispositivos actúan como clientes y servidores a la vez. Es sencilla y económica, pero no escalable ni segura para entornos grandes.

 **4. What type of traffic occurs when a packet is sent to all devices in a local network?**

¿Qué tipo de tráfico se genera cuando un paquete se envía a todos los dispositivos de una red local?

Opciones:

- A. Unicast
- B. Multicast

C. Broadcast

D. Anycast

 **Respuesta correcta:** C. Broadcast

Explicación:

El **broadcast** se usa para enviar mensajes a todos los hosts de una red (por ejemplo, ARP requests). Un exceso de tráfico broadcast puede causar congestión y degradar el rendimiento.

 **5. Which layer of the hierarchical network model routes traffic between VLANs and applies access policies?**

¿Qué capa del modelo jerárquico enruta el tráfico entre VLANs y aplica políticas de acceso?

Opciones:

A. Access Layer

B. Core Layer

C. Distribution Layer

D. Network Layer

 **Respuesta correcta:** C. Distribution Layer

Explicación:

La **Distribution Layer** conecta la capa de acceso con la de core. Implementa enrutamiento entre VLANs, aplica políticas de seguridad y controla el flujo del tráfico interno.



6. Which modern data center architecture connects every leaf switch to all spine switches for redundancy?

¿Qué arquitectura moderna de centro de datos conecta cada switch leaf con todos los spine para mayor redundancia?

Opciones:

A. Ring

B. Spine-Leaf

- C. Mesh
- D. Collapsed-Core

 **Respuesta correcta:** B. Spine-Leaf

Explicación:

En una **spine-leaf topology**, cada leaf tiene un enlace hacia todos los spines, eliminando cuellos de botella y mejorando la latencia. Es el estándar actual en data centers modernos.

7. What technology separates the control plane from the data plane for centralized network management?

¿Qué tecnología separa el plano de control del plano de datos para una gestión centralizada de red?

Opciones:

- A. VLAN
- B. MPLS

C. SDN (Software-Defined Networking)

D. VPN

 **Respuesta correcta:** C. SDN (Software-Defined Networking)

Explicación:

SDN permite que las decisiones de enrutamiento se tomen en un **controlador centralizado**, que programa los switches o routers sin configuración manual en cada dispositivo.

 **8. Which network type is designed specifically to connect servers to storage systems?**

¿Qué tipo de red está diseñada específicamente para conectar servidores a sistemas de almacenamiento?

Opciones:

A. PAN

B. SAN

C. LAN

D. CAN

 **Respuesta correcta:** B. SAN (Storage Area Network)

Explicación:

Una **SAN** conecta servidores a almacenamiento de alta velocidad mediante protocolos como **Fibre Channel** o **iSCSI**, ofreciendo baja latencia y gran capacidad.

9. Which WAN technology uses labels to route packets instead of IP addresses?

¿Qué tecnología WAN utiliza etiquetas para enrutar paquetes en lugar de direcciones IP?

Opciones:

A. MPLS

B. Frame Relay

C. ATM

D. VPN

 **Respuesta correcta:** A. MPLS (Multiprotocol Label Switching)

Explicación:

MPLS enruta paquetes basándose en etiquetas (labels) en lugar de direcciones IP, mejorando el rendimiento y permitiendo priorización del tráfico (QoS).

 **10. Which topology combines two or more different topologies to take advantage of their strengths?**

¿Qué topología combina dos o más topologías distintas para aprovechar sus ventajas respectivas?

Opciones:

A. Bus

- B. Hybrid
- C. Mesh
- D. Ring

 **Respuesta correcta:** B. Hybrid

Explicación:

Una **topología híbrida** combina elementos de diferentes diseños (por ejemplo, *star-bus*). Ofrece equilibrio entre rendimiento, escalabilidad y tolerancia a fallos.

26. Conclusión

Podemos observar que los fundamentos de este capítulo sientan las bases para todo el aprendizaje posterior en redes.

La comprensión de los **tipos de red, arquitecturas y topologías** no solo es esencial para el examen *CompTIA Network+*, sino también para el diseño de infraestructuras reales, donde la **virtualización, segmentación y automatización**

marcan la diferencia entre una red estática y una red moderna, dinámica y segura.



Fin del Capítulo 1 – Introduction to Networks